Government Information Quarterly 39 (2022) 101718

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Internet voting in Estonia 2005–2019: Evidence from eleven elections

Piret Ehin[a], Mihkel Solvak[a], Jan Willemson[b,*], Priit Vinkel[b]

[a] University of Tartu, Ülikooli 18, 51003, Tartu, Estonia
[b] Cybernetica AS, Narva mnt 20, 51009 Tartu, Estonia

ARTICLE INFO

Keywords:
Internet voting
i-voting
e-voting
Elections
Trust
Technology adoption
Vote verification

ABSTRACT

Internet voting is a highly contested topic in electoral studies. This article examines Internet voting in Estonia over 15 years and 11 nation-wide elections. It focuses on the following questions: How is Internet voting organized and used in Estonia? How have the Estonian Internet voting system and its usage evolved over time? What are the preconditions and consequences of large-scale deployment of Internet voting? The results suggest that the rapid uptake and burgeoning usage rates reflect the system's embeddedness in a highly developed digital state and society. Through continuous technological and legal innovation and development, Estonia has built an advanced Internet voting system that complies with normative standards for democratic elections and is widely trusted and used by the voters. Internet voting has not boosted turnout in a setting where voting was already easily accessible. Neither has it created digital divides: Internet voting in Estonia has diffused to the extent that socio-demographic characteristics no longer predict usage. This, combined with massive uptake, reduces incentives for political parties to politicize the novel voting mode.

1. Introduction

New technologies have the power to transform the act central to democracy – voting. As daily transactions have increasingly migrated to the Internet, the notion that voters need to go to a polling station in person in order to cast a vote seems increasingly questionable. The global pandemic, which has delayed and disrupted democratic elections worldwide (International Institute for Democracy and Electoral Assistance, 2021), has provided urgency to debates about new and alternative modes of voting (Krimmer et al., 2021a). Yet, despite the numerous advantages of Internet voting (i-voting) including improved accessibility, convenience, speed, and reduced cost, voting in most countries remains a staunchly analogue affair. In fact, several countries have recently halted or abandoned trials of Internet voting systems (BBC, 2014; Duenas-Cid et al., 2020; Kuenzi, 2019; Reuters, 2017), and widespread concerns about the integrity and security of any form of electronic voting have amplified calls to rely on nothing but tried-and-true paper ballots.

In this context, the case of Estonia deserves special attention. The first country in the world to institute Internet voting in nation-wide elections, Estonia has, since 2005, enabled all voters to cast ballots from any Internet-connected computer located anywhere in the world. Over the course of the past 15 years, Estonian voters have cast i-votes in four national and three European Parliament elections, in addition to four nation-wide local elections. Internet voting has become widespread and popular: in the most recent Estonian elections (2019 European Parliament contests), nearly a half of all ballots cast were i-votes.[1] An analysis of i-voting in Estonia offers insights into a bold electoral experiment, providing valuable evidence for anyone contemplating Internet voting, or, more broadly, the potential of technology to transform democracy.

The objective of this article is to describe and explain the functioning of the Estonian Internet voting system. Specifically, the paper seeks to answer the following research questions:

i How is Internet voting organized and used in Estonia?
ii How have the Estonian Internet voting system and its usage evolved over time?
iii What are the preconditions and consequences of large-scale deployment of Internet voting?

To answer these questions, we conduct a case study examining Internet voting in Estonia over a period of 15 years (2005–2019) and 11 nation-wide elections.

* Corresponding author.
E-mail addresses: piret.ehin@ut.ee (P. Ehin), mihkel.solvak@ut.ee (M. Solvak), jan.willemson@cyber.ee (J. Willemson), priit.vinkel@gmail.com (P. Vinkel).

[1] https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

https://doi.org/10.1016/j.giq.2022.101718
Received 30 April 2021; Received in revised form 13 December 2021; Accepted 28 May 2022
Available online 16 June 2022

Such an analysis fills a significant gap in the literature. While the Estonian experiment has been studied before from a number of angles, a comprehensive yet accessible up-to-date overview of Internet voting in Estonia is currently missing in the scholarly literature. The most recent article providing a general overview of the Estonian i-voting system was published more than ten years ago and is based on data from the very first parliamentary election in which i-voting was deployed (Alvarez, Hall, & Trechsel, 2009). While subsequent contributions have examined specific aspects of Estonian i-voting (Heiberg et al., 2011; Heiberg & Willemson, 2014a; Solvak & Vassil, 2018; Vassil et al., 2016; Vassil & Weber, 2011), they do not describe the overall set-up of the system. This has resulted in a situation where a reader who seeks to understand how Estonian i-voting works has to scrape together the picture from a wide variety of dispersed sources. Furthermore, the rapid evolution of the technological and legal basis of the Estonian i-voting system, along with burgeoning usage rates, call for renewed efforts to analyze and assess.

This article is structured in seven sections. We define the phenomenon of interest and provide a brief overview of the global context, before introducing our methods and data. Turning to our case, we provide an overview of i-voting in Estonia, focusing on adoption and enabling conditions, the legal and technical basis, as well as provisions for privacy and transparency. The next section examines usage rates and patterns, as well as trust as a precondition for usage. We cover the evolving positions of Estonia's main political parties before summarizing the findings and offering five main takeaways from the Estonian experience with remote Internet voting.

2. Concept and global context

Remote Internet voting is a system of voting where the voters cast their votes from a remote Internet-enabled computer or another access device. Neither the device used for voting nor the physical environment of voting are under the control of election officials: voters can cast a ballot from home, work, their favorite cafe, a hotel room abroad, or on board an intercity train. Remote Internet voting should not be confused with other types of electronic voting, such as the use of standalone electronic voting machines, voting kiosks, or simply using the Internet for transmitting and tabulating results. This article uses the terms 'Internet voting' and 'i-voting' to denote remote Internet voting.

I-voting has a number of advantages. It eliminates obstacles to electoral participation that stem from distance, transportation, terrain, and weather. It facilitates participation and increases accessibility, including for voters with health issues and disabilities, citizens living in remote areas, and people who care for small children or the elderly. Not having to go to a polling station saves voters time and money. I-voting is compatible with modern mobile lifestyles that comprise travel, migration, and transnationalism. Internet voting reduces costs to electoral authorities by reducing the need to deploy and operate physical polling stations (Krimmer et al., 2021b), and makes the tallying, tabulation and delivery of voting results faster (Krimmer, 2012). I-voting has been seen as a remedy to low and decreasing electoral participation rates (Alvarez & Hall, 2004), especially among young voters. Finally, providing a variety of voting channels is seen as a way to offer better services to the electorate (Germann & Serdült, 2017; Solvak & Vassil, 2018).

Inspired by the potential of Internet voting to increase participation and enhance the efficiency of elections, a number of countries have explored and trialled Internet voting systems since the early 2000s (for a comprehensive, although somewhat dated overview see Krimmer et al., 2007). The State of Geneva in Switzerland, which had extensive experience with postal voting, introduced i-voting in 2003. Other Swiss cantons followed suit: in over 300 trials held to date, fifteen cantons have allowed certain groups of citizens to vote online (Federal Chancellery of the Swiss Confederacy, 2021; Germann, 2021; Gibson et al., 2016). However, the share of i-votes remained low at around 2 per cent nationwide, and in 2019, e-voting was suspended after the discovery of security flaws in the voting systems used (Culnane et al., 2019). Norway experimented with Internet voting in elections held in 2011 and 2013 but abandoned the program amidst fears that vote anonymity was not guaranteed (Bull et al., 2018). Internet voting was trialled in local elections in the United Kingdom between 2002 and 2007, before being abandoned. France allowed Internet voting in legislative elections for overseas territories since 2012 but stopped this practice due to cyber attack fears in 2017 (Reuters, 2017). While some European countries, such as Lithuania, are planning to roll out i-voting systems for overseas voters (LRT English, 2020), others, such as Finland, remain skeptical of i-voting, as working groups convened by governments argue that the risks outweigh the benefits (Finnish, 2017). The small autonomous Finnish islands of Åland scrapped their plans for using i-voting in their local elections due to security reasons only a couple of days before their election period (Duenas-Cid et al., 2020; Krimmer et al., 2019).

Outside of Europe, Internet voting has been used in municipal elections in the Canadian provinces of Ontario and Nova Scotia (Goodman & Gabel, 2020). Several US states, including New Jersey, Delaware and West Virginia, allow overseas, military and disabled voters to cast a ballot over the Internet, and several more are considering the possibility (Specter & Halderman, 2021). In Asia, Pakistan has recently implemented small-scale trials of Internet voting for overseas voters (IVTF, 2018); in India, trials have been conducted in the state of Gujarat (The Indian Express, 2015). In Australia, two large regions, New South Wales ad Western Australia, allow certain groups of voters, including disabled and absentee voters, to cast remote Internet votes in regional elections (Electoral Commission, 2020).

As confirmed by the brief overview provided above, most experiments with remote Internet voting in the world have been limited in scope, have occurred at the sub-national level, and more often than not, have been discontinued. The reasons for discontinuation are diverse, ranging from technology failures, risk assessments and expert warnings to questions of political will and calculations of expected electoral gains and losses for specific political actors. Concerns about privacy and integrity typically top the list of counterarguments to electronic voting in general and Internet voting in particular. While unrelated to remote Internet voting, problems with electronic voting machines used in the United States and elsewhere have negatively impacted the reputation of electronic voting (Appel et al., 2008, 2009; Aviv et al., 2008; Bannet et al., 2004; Dill et al., 2003; Feldman et al., 2007; Wolchok et al., 2010). Internet voting, furthermore, is associated with specific risks that stem from the fact that voting takes place at an uncontrolled location and electronic ballots are transferred via the Internet. Potential risks include threats to voters computers, attacks against election infrastructure, procedural oversights and implementation errors, voter fraud and the use of coercion (Krips & Willemson, 2019; Küsters & Müller, 2017; Willemson, 2018).

I-voting systems developed around the world differ greatly in terms of whether and how effectively they mitigate these and other risks (Jafar & Ab Aziz, 2020; Marky et al., 2018; Park et al., 2021). Risk analysis of Internet voting is a highly complex topic and providing a comprehensive overview of the relevant considerations is well beyond the limits of this paper. It is important to note, however, that no practical system in the world is risk-free, and that there are trade-offs between desirable properties of electoral systems such as security, accessibility, accuracy, verifiability, anonymity, transparency and cost-effectiveness (Willemson, 2018; Wilson, 2019). We refer an interested reader to recent reports on the topic (Applegate et al., 2020; Vote Foundation, 2015).

Growing interest in electronic voting, along with an acknowledgement of the risks involved, has led to international efforts to define standards for e-enabled elections. Council of Europe Recommendation rec(2004)11 (Council of Europe, 2004) and the updated rec(2017)5 (Council of Europe, 2017) stipulate the legal standards for electronic voting, including universal, free, and secret suffrage, along with procedural safeguards such as transparency, verifiability, accountability, reliability and security. These documents also set operational and technical standards pertaining to accessibility, interoperability, system

Table 1
General statistics of Estonian Internet voting. (Source: State Electoral Office)

	2005	2007	2009	2009	2011	2013	2014	2015	2017	2019	2019
	local	national	EP	local	national	local	EP	national	local	national	EP
Eligible voters	1059292	897243	909628	1094317	913346	1086935	902873	899793	1100647	887420	885417
Participating voters	502504	555463	399181	662813	580264	630050	329766	577910	586519	565045	332859
Voter turnout	47.4%	61.9%	43.9%	60.6%	63.5%	58.0%	36.5%	64.2%	53.3%	63.7%	37.6%
I-voters	9317	30275	58669	104413	140846	133808	103151	176491	186034	247232	155521
I-votes cancelled	30	32	55	100	82	146	46	162	163	191	73
I-votes counted	9287	30243	58614	104313	140764	133662	103105	176329	185871	247041	155448
Multiple i-votes	364	789	910	2373	4384	3045	2019	4593	4527	6340	2555
I-voters among eligible voters	0.9%	3.4%	6.5%	9.5%	15.4%	12.3%	11.4%	19.6%	16.9%	27.9%	17.6%
I-voters among participating voters	1.9%	5.5%	14.7%	15.8%	24.3%	21.2%	31.3%	30.5%	31.7%	43.8%	46.7%
I-votes among early votes	7.2%	17.6%	45.4%	44.0%	56.4%	50.5%	59.2%	59.6%	60.6%	71.4%	69.4%
I-votes cast abroad among i-votes	n/a	2.0%	3.0%	2.8%	3.9%	4.2%	4.7%	5.7%	4.1%	6.3%	5.5%
No. of countries i-votes were cast from	n/a	51	66	82	105	105	98	116	115	143	109
Share of verified votes	n/a	n/a	n/a	n/a	n/a	3.4%	4.0%	4.3%	4.0%	5.3%	4.1%
Share of Mobile-ID use	n/a	n/a	n/a	n/a	1.9%	8.6%	11.0%	12.2%	23.8%	29.2%	30.1%

operation, security, audit and certification. To facilitate the implementation of the recommendation, the Council has adopted guidelines for certification of e-voting systems and on transparency of e-enabled elections (Binder et al., 2019). The latter document emphasizes the importance of trust, arguing that e-voting systems can only be introduced "if voters have trust and confidence in their current electoral system" and calling on states to "do their utmost in order to ensure that [trust] is preserved" notably by ensuring transparency (Council of Europe, 2011).

Against the global backdrop of limited and halting experiments with i-voting, the case of Estonia constitutes a striking exception. Having first deployed i-voting in nationwide local elections in 2005, Estonia remains the only country in the world that offers all voters the option to cast an electronic ballot remotely in all nationwide elections. Subsequent sections of this article present a comprehensive overview of the Estonian i-voting system and its use by the voters.

3. Methods and data

This study is a case study of Internet voting in Estonia that combines the goals of description and explanation. The case study method is suitable for investigating a contemporary phenomenon in depth and in its real-world context (Yin, 2018). The case analyzed in this study is the Estonian Internet voting system over a period of 15 years (2005–2019). Eleven elections took place during this period, including four national and three European Parliament elections, in addition to four nationwide local elections. Considering that no other county in the world enables all voters to vote online, and no other country comes close to Estonia's i-voting usage rates, the Estonian Internet voting system constitutes an extreme or unusual case (Gerring, 2008). This justifies a single case design (Yin, 2018). Furthermore, building on Stake (1995), we classify our case study as an intrinsic case study, the purpose of which is to better understand a unique case in depth, rather than to understand some generic phenomenon or build theory. The results of an intrinsic case study provide a holistic view of how and with what results Internet voting can be deployed on a large scale and become a regular, widely accepted voting mode.

Case studies typically rely on multiple sources of evidence – a strategy that enhances data credibility and trustworthines (Yin, 2018). This study uses data from a range of sources, including legal acts, court judgments, reports by election monitoring organizations, media articles, official electoral statistics, and individual-level survey data from the Estonian Internet voter study 2005–2019 (Johan, 2019), which covers all 11 elections in which i-voting has been available. Each post-election survey had a sample of roughly 1000 eligible voters; the combined dataset consists of 11,059 interviews. For information on sampling and interview methods, see Appendix A.

4. I-voting in Estonia

Estonia (population: 1.3 million) is a competitive multi-party democracy that ranks very high in terms political rights and civil liberties (Freedom House, 2020). Elections to the 101-member national parliament, Riigikogu, are held every four years. Local government councils, which have a term of four years, are also elected in nation-wide elections. Since Estonia joined the EU in 2004, it has held European Parliament elections every five years. The electoral system is a form of open-list proportional representation: voters cast a vote for a candidate on a party list, and parties get seats proportionally to the share of the vote received. Voting age is 18, except in local elections, where 16- and 17-year olds have been able to vote since 2017. The list of voters is compiled based on the Population Register; voter registration does not require any action on the part of the citizen. Arrangements for conventional paper voting are as follows. Election day is Sunday. Early voting is available during a designated week. Voters with special needs can get the ballot box delivered to their home or residence. Voters permanently or temporarily residing abroad (numbering over 80,000 in recent elections) can vote at an Estonian diplomatic representation or order a mail-in ballot.

Internet voting has been used in national, European and local elections since 2005. An optional alternative to conventional paper voting, i-voting is available during a designated early voting period (from the tenth until the fourth day before Election Day). Voters can cast a ballot from any Internet-connected computer from any location in the world. From the election web page, voters first download a voting application and launch it in their own computers. Next they authenticate themselves using the Estonian ID-card or a mobile-ID, view the list of candidates running in their district, make their choice, encrypt it and confirm their vote with a digital signature. The entire process takes less than two minutes on average (Heiberg et al., 2015). Notably, voters can change their electronic votes an unlimited number of times during the early voting period, with each new vote annulling the previous ones. Voting at the polling station during the early voting period invalidates the ballot cast over the Internet. These provisions are in place in order to protect the secrecy of voting: a voter who was coerced or intimidated to vote a certain way can cast a new ballot and overwrite their previous vote. Until 2021, i-voters could not cast a ballot on Election Day, as their names were removed from the relevant voter lists. From 2021 on, i-voters can cast a paper ballot on Election Day, thereby invalidating their electronic vote.

4.1. Adoption and enabling conditions

The Estonian government announced the idea to introduce Internet voting in 2001. The same year, the first technical analyses were published by Estonian academics (Lipmaa & Mürk, 2001; Tammet & Krosing, 2001). The interest in i-voting was driven by the hope to increase voter turnout, attract younger voters, and make voting more convenient (OSCE/ODIHR, 2007, p. 9). After a security analysis conducted in 2003 (Ansper et al., 2003), the national electoral committee adopted a concept paper developed by a designated project group, and following a public tender, awarded a contract to develop an i-voting solution to an Estonian software development company Cybernetica. Legislation enabling Internet voting was first adopted in 2002. Internet voting was first deployed in local elections held in October 2005 in which the novel voting mode was used by 1.9 per cent of participating voters (see Table 1).

The decision to develop a system of i-voting must be viewed in the context of preceding steps that laid the foundation for what has become one of the world's most advanced systems of e-governance (European Commission, 2020; United Nations, 2020). The restoration of Estonia's independence in 1991, following a half-century of Soviet domination, coincided with the period of fast computerisation and Internet becoming available for general use. In late 1990s, two important political decisions were taken that later became the two pillars of the Estonian digital society – creating the X-Road data exchange middleware, and establishing a national Public Key Infrastructure (PKI) together with a strong cryptographic authentication token, the Estonian ID-card. Both of these were first deployed in early 2000s (Kalja et al., 2005).

The Estonian ID-card is a state-issued identity document that is mandatory for Estonian citizens and citizens of the European Union who are permanently residing in Estonia. Issued since 2002, the card is equipped with a smart chip which provides advanced electronic functionality such as secure authentication and digital signatures. Another mechanism of electronic identification, smartphone SIM-card based mobile-ID, was introduced in 2007. The mobile-ID and the digital functionalities of the ID-card are widely used on a daily basis to access thousands of public e-services and to give legally binding digital signatures. By early 2021, both the total number of electronic identifications using the Estonian ID-card and the total number of digital signatures given by the residents of Estonia had surpassed 1 billion.[2] For a comprehensive overview of the Estonian ID-card and its ecosystem (see Martens, 2010; Parsovs, 2021).

The capacity of ID-cards to strongly bind digital and physical identities allowed the Estonian government to completely rethink public services. Applying for benefits, filing taxes or renewing a driver's licence became something that people were able to do from the comfort of their home instead of going to an office. The X-Road data exchange layer enabled public and private sector e-service information systems to connect and transfer data, functioning as an integrated whole. This digital infrastructure is used daily for hundreds of thousands of interactions across all levels of the Estonian state, the private sector and society, including in banking, taxation, health, and education.

The digital competences, capabilities and attitudes of Estonia's residents have evolved in step with the evolution of the digital state. The share of Internet users in the 16–74 age group has grown from 58 per cent in 2005 to 89 per cent in 2020; in the 16–44 age group, 98 percent of people used the Internet daily or almost daily in 2020 (Statistics Estonia, 2021a). The share of households with an Internet connection has increased from 37 per cent in 2005 to 90 per cent in 2020 (Statistics Estonia, 2021b). Mobile broadband penetration is among the highest in the world, standing at 158 subscriptions per 100 inhabitants in 2020 (OCED, 2020).

Estonian e-governance solutions are not only widely used, but also widely trusted by the general public. Survey data from 2020 suggest that 82 per cent of residents trust Estonian e-governance and digital services; among working-age respondents, the respective figure was 88 per cent (Raag, 2020). The primary state institution responsible for the nation's digital infrastructure – the State Information System Authority – regards earning and maintaining public trust as a central pillar of digital service design and governance (State Information System Authority, 2020). It seems to succeed at its mission: Estonians' high trust in digital government survived the ID-card security crisis that hit the country in 2017 when it was discovered that the ID-card chip, produced by a multinational company Infineon, had a security vulnerability that affected around 800,000 Estonian ID-cards in addition to millions of cards used worldwide (Estonian Police and Border Guard Board, 2017; Nemec et al., 2017). Estonian authorities resolved the crisis by developing a software update which made it possible to bypass the vulnerability without replacing the affected cards (Parsovs, 2020).

In sum, the existence of a highly developed national digital infrastructure is a major enabling condition and a key to understanding Estonian exceptionalism in the realm of Internet voting.

4.2. The evolving legal basis

Estonia has a comprehensive legal and regulatory framework that facilitates i-voting. The Identity Documents Act, adopted in 1999, has evolved to include detailed provisions for digital identity cards, including digital identification via mobile-ID. The Digital Signatures Act, adopted in 2000, regulates the use of legally binding digital signatures, along with the provision of certification and time-stamping services. The Population Register Act and the Personal Data Protection Act regulate the use of data recorded in the Population Register, the state's main database containing information on all citizens and residents of Estonia.

Provisions for Internet voting were first included in a series of electoral acts adopted in 2002, including the Riigikogu Election Act, Local Government Council Election Act, and the Referendum Act. The laws stipulated an early voting period during which electronic votes can be cast, and included the basic provisions enabling i-voting with the use of digital ID-cards. The right to change one's i-vote (by casting a paper ballot or a new i-vote) was included, along with detailed clauses on vote counting, including cancellation of multiple votes. These legal provisions allowed electoral authorities to start preparations for introducing i-voting in the 2005 local elections.

Over the course of two decades, i-voting legislation and technical regulations have been developed through a series of amendments which reflect both domestic visions for improving the system as well as recommendations made by the Office for Democratic Institutions and Human Rights (ODIHR) of the Organization for Security and Cooperation in Europe (OSCE). Following invitations by the Estonian government, OSCE/ODIHR election assessment missions or smaller expert teams have observed and reported on all four Riigikogu elections in which i-voting has been used (2007, 2011, 2015, 2019) (OSCE/ODIHR, 2015, 2019).

The first OSCE/ODIHR report, focusing on the 2007 elections, was the most critical of the four, emphasizing the need to introduce more comprehensive testing and auditing of the i-voting system and to increase oversight by political parties and the civil society. The 2011 report found that the conduct of Internet voting is widely trusted, but called for "further improvement of the legal framework, oversight and accountability, and some technical aspects of the Internet voting system" (OSCE/ODIHR, 2011, p. 1). In response, Estonia amended the electoral acts to set up an Electronic Voting Committee under the auspices of the Electoral Committee, tasked with organizing Internet voting. The requirement of conducting pre-election tests and post-election audits of the i-voting system was added. In addition, the amendments included the requirement that, from 2015 on, voters must have the possibility to verify that their vote has reached and is stored at the

[2] https://www.id.ee/en/

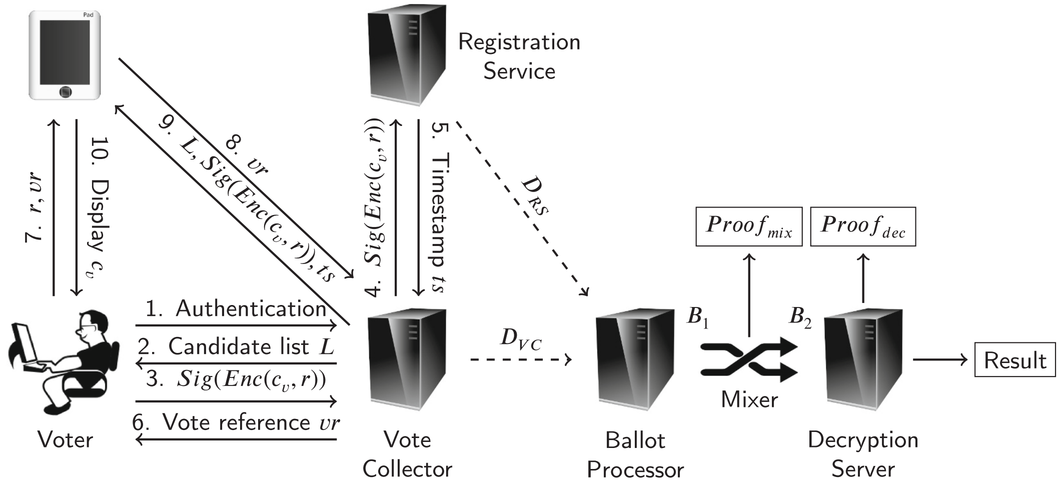

Fig. 1. The general scheme of Estonian internet voting since 2017.

central server of the elections and reflects the choice of the voter correctly. Vote verification with a second device, such as a smart phone, was introduced ahead of the 2015 Riigikogu elections.

The 2015 OSCE/ODIHR report argued that i-voting was "administered efficiently and in line with the legal framework" while calling for additional measures to enhance transparency and accountability (OSCE/ODIHR, 2015, p. 1). The Riigikogu started a new set of deliberations in 2015 with the intention to increase verifiability and transparency by looking at election administration in a holistic manner. The entire system of election administration was revamped by separating the oversight duties of the National Electoral Committee (NEC) from election management duties which were to be performed by a new institution – the State Electoral Office (SEO) under the Chancellery of the Parliament. Moreover, i-voting was more closely integrated into the state e-governance ecosystem by separating the technical duties of the vote collecting agent from the election management duties of the SEO. In addition, an updated technological framework for i-voting was developed and used for the first time in the 2017 local elections (see Section 4.3). These changes were welcomed by the OSCE/ODIHR, which, in its report on the 2019 Riigikogu elections, concluded that "the current design of the Internet voting system constitutes a significant improvement over earlier versions", notably in terms of the system's integrity and secrecy properties (OSCE/ODIHR, 2019, p. 1). The report dedicates only about two pages to Internet voting, suggesting that the SEO develop strategies to mitigate the risk of internal attacks or disinformation campaigns and further improve quality assurance and auditing processes.

The restructuring of election administration and oversight was a direct consequence of the increased complexity associated with the deployment and use of i-voting. The founding of the SEO in 2017 was driven by the growing number and complexity of technical tasks and challenges stemming from the increasingly widespread use of i-voting (Riigikogu, 2015). Prior to organizational reforms, election management duties were carried out by a 7-member collective body, the NEC, the members of which represented different state offices and held their position in addition to their every-day jobs. With the reforms, the SEO became a specialized independent institution while the NEC took on oversight functions. In addition to performing general election management duties, the SEO functions as hub in the network of governmental agencies that provide technical support to organizing elections (McBrien, 2020).

Estonian courts have scrutinized and upheld the constitutionality of i-voting, ruling that legal provisions on Internet voting meet the constitutional requirement to hold free, general, uniform and direct elections in which voting is secret. Reviewing a petition submitted by the President of the Republic, the Estonian Supreme Court ruled in 2005 that the possibility to change one's electronic vote during the early voting period does not violate the principle of uniformity of elections. Furthermore, the Court argued that the option of changing one's electronic vote constitutes an additional guarantee of the freedom to vote and secret voting, as it "renders the influencing of the will of a voter by illegal means useless and pointless" and provides an "essential remedy for restoring the secrecy of voting" to any person who feels that the privacy of their vote was compromised for any reason (Supreme Court of Estonia, 2005; Vinkel, 2015). Additionally, the highest court has found in judgements on electoral complaints and appeals that the conduct of i-voting by the electoral management body has followed prescribed legal provisions and procedures and that there have not been any serious incidents that could have affected election results (Supreme Court of Estonia, 2011, 2013, 2017). However, there is still room for improvement, as the Supreme Court ruled in 2019 that additional technical and procedural provisions related to i-voting should be regulated by law rather than by sub-legal acts by the National Electoral Committee or the SEO (Supreme Court of Estonia, 2019a, 2019b).

4.3. *Technical overview*

The general scheme of Estonian Internet voting (code-named IVXV) in use since 2017 is depicted in Fig. 1. We refer to State Electoral Office of Estonia (2017), Heiberg and Willemson (2014b), and Heiberg et al. (2016) for further technical details.

The voter starts the process by authenticating herself (1) from the PC-based voting application to the Vote Collector server (VC) using an electronic identity mechanism (typically ID-card or mobile-ID). The server replies with the list of candidates L (2) corresponding to the voter's electoral district. The voter selects her favourite candidate c_v, encrypts her vote with the Decryption Server's public key, signs the cryptogram with her eID and sends the result back to VC (3). Note that all the encryptions are randomised so that votes given to the same candidate would look different. For that purpose, encryption randomness r is used in step (3).

In order to make sure that VC does not accidentally or maliciously drop some of the votes, the protocol then mandates committing the vote to a separate Registration Service (4). This service returns a timestamp ts (5) certifying the fact that the vote indeed has been committed somewhere outside VC.

Next, the voter has an option of verifying the vote. The objective of individual verification is to establish two facts. First, the voter can make sure that the vote under encryption is indeed what she intended and not manipulated by, say, malware residing on her PC. Second, the voter can

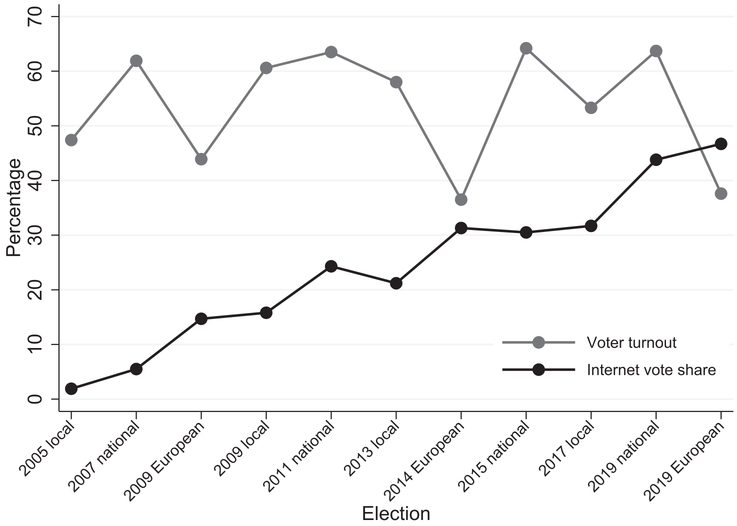

Fig. 2. Share of Internet votes and voter turnout (2005–2019) (Data source: State Electoral Office).

check the timestamp *ts* to check that her vote was correctly committed outside VC, and hence VC can not delete it without anyone noticing.

To facilitate verification, the VC provides a vote reference *vr* to the voting application (6). Because we want to ensure vote integrity even in the presence of a malicious attacker in the voter's PC, verification should be conducted via an independent device. For that, Estonian voters can use their mobile devices. The mobile device is provided the *vr* via optical close-range channel, namely QR-code (7). The mobile device makes a query to VC using *vr* (8) and receives back the list of candidates L, the signed-encrypted vote and the timestamp *ts* (9).

Neither the voter's PC nor the mobile device have access to the Decryption Server's private key, meaning that the mobile verification app cannot decrypt the vote directly. Luckily, having access to encryption randomness is also sufficient for decryption. This is why r is also supplied to the mobile device on step (7).

Now the mobile device can verify the timestamp and the signature on the vote, and decrypt and display the candidate c_v on its screen (10). The voter will make the comparison with her original intent in her head, raising alarm and/or revoting if the result does not match.

After the voting period is over, the ballots will be prepared for tallying. The vote sets D_{VC} and D_{RS} stored at VC and the Registration Service, respectively, are transferred over air gap to the offline Ballot Processor unit. The latter checks that all the votes in D_{VS} have correct timestamp commitments in D_{RS}, removes all but the last ones of the revotes, and removes the signatures to make the votes anonymous.

To allow for independent auditability of the tally process without breaching vote anonymity, the resulting ballot list B_1 is sent through a Mixer component, producing an output ballot list B_2 together with a cryptographic proof of correct mixing. The vote cryptograms in the list B_2 will finally be decrypted using the Decryption Server's private key, producing the end result and the cryptographic proof of correct decryption.

4.4. Privacy and transparency

The Estonian Internet voting scheme described in Section 4.3 is designed to provide a reasonable balance between voter privacy and system transparency. The vote is encrypted with a public key, with the corresponding private key being available only to the Decryption Server. If the voter was unable to express her preference freely (e.g. due to coercion) when casting the vote, she can cast another vote (either electronically or in the polling station) later, and only the last vote will be counted. The voter can also verify that her vote reached the Collector server and has been committed to the Registration Service. Note, however, that the voter *cannot* obtain a strong proof that her vote was included in the final tally as such a proof could potentially be used for vote selling. Thus, evidence created in the process of i-voting is comparable to the evidence that could be obtained while voting at the polling station. Creating protocols that would provide better evidence for the i-voter while not enabling vote selling is currently an active area of research.

Even though full public server-side auditability is currently not possible, designated auditors can still verify the correctness of server-side operations, hence providing a level of assurance similar to that of paper voting. Two of the critical system components (Mixer and Decryption Server) export independently verifiable cryptographic proofs of correct operation. Independent auditors are required by law to verify the integrity of the system as well as the compliance of the main procedures with the rules and regulations, and perform a data audit certifying the correctness of data processing. This is the highest level of transparency achievable with currently known practically applicable methods.

Everyone has the right to observe the elections, including the activities, procedures and processes related to i-voting such as the counting of i-votes. To ensure that observers understand the relevant processes, rules and norms, the SEO organises observers' training before each election.

In addition, almost all of the source code of the applications used to run i-voting is available openly.[3] The only notable exception is the source code of the official voting application. As this is the application operating in an environment that is potentially the most hostile (the voter's PC), keeping its source closed is considered to be a justified defense mechanism. However, the correctness of the code's operation can be ensured by using the (open-source) vote verification mobile app. Recently, an independent voting application working on a much more limited microcontroller platform has also been developed (Farzaliyev et al., 2021).

5. I-voting in Estonia: usage and trust

5.1. Usage rates and patterns 2005–2019

Over the course of 1 years, the number of i-voters as well as the share

[3] https://github.com/vvk-ehk/ivxv

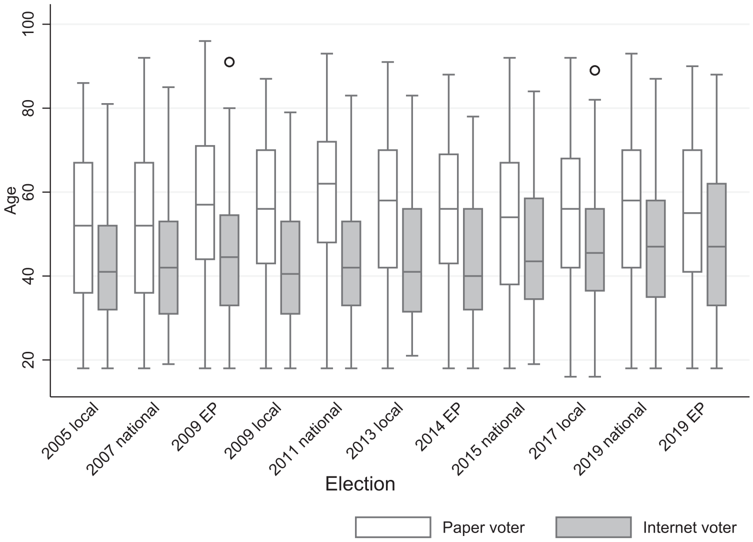

Fig. 3. Age structure of paper and Internet voters 2005–2019 (Source: Estonian Internet voter study 2005–2019).

of electronic votes have grown steadily (see Fig. 2 and Table 1).

In the 2005 local elections, fewer than 10,000 voters voted over the Internet; the share of i-votes out of all votes was a mere 1.9 per cent. Over the next four years, the number of i-voters increased tenfold: 104, 413 voters cast an electronic ballot in the 2009 local elections. In 2011, almost 141, 000 voters cast an i-vote in the general elections, with the share of e-votes approaching a quarter of all votes cast. In March 2019 Riigikogu elections, nearly a quarter million voters cast an electronic ballot, with i-votes constituting 43.8 per cent of all votes. In European Parliament elections held in May 2019, the share of i-votes reached 46.7 per cent. A continuation of this trend would mean that in the 2023 general elections, the majority of votes cast will be electronic votes.

Contrary to expectations, Internet voting has not boosted turnout. Although some estimates suggest that Internet voting has increased turnout by up to 2.6 per cent in local elections (Trechsel & Vassil, 2011, p. 58), others have demonstrated that the main effect is not an increase but the stabilization of turnout at the level of 63–64 per cent in national elections (Solvak & Vassil, 2018). The expected turnout increase seems, in hindsight, to have been a misplaced hope. Instead, a “bottleneck” effect is apparent where the probability of using Internet voting is lowest among the population segment least likely to participate in elections (Solvak & Vassil, 2016; Vassil & Weber, 2011), i.e. usage probability is paradoxically lowest in a segment of the electorate where mobilization would make the greatest difference. In other words, i-voting does not appear to be mobilizing non-voters.

Aside from unchanged turnout figures, a number of patterns and features of i-voting deserve attention. First, i-voting has boosted the popularity of early voting: it has been the dominant mode of early voting since 2011. Before the introduction of i-voting, about 21 per cent of votes cast in a national election were early votes. In the 2019 Riigikogu elections, the respective figure was 61.3. In the two elections held in 2019, about 70 per cent of the early votes were electronic votes (see Table 1). With nearly two-thirds of the the voters casting their votes well before Election Day, the temporal logic of elections has changed, and the significance of Election Days lies more in the announcement of the results rather than the act of voting itself. The prevalence of early voting distinguishes Estonia from the European mainstream: most EU countries do not allow early voting (Heinmaa, 2020).

Second, i-voting statistics include information about the unusual practice of casting multiple votes in the same election. As explained above, Estonian voters have the right to change their i-votes an unlimited number of times during the early voting period. They can also overrule their electronic vote by casting a paper ballot during the early voting period. Over the past decade, the number of voters who cast multiple electronic ballots has varied from 2019 in the 2014 European Parliament elections to 6340 in the 2019 general election (see Table 1). Casting multiple votes is fairly rare: 98 per cent of i-voters vote once, 1–2 per cent vote twice, and only a couple of hundred voters cast three or more ballots in a given election (Heiberg et al., 2015; Solvak & Vassil, 2016). Casting both a paper vote and an electronic vote during the early voting period – which results in the cancellation of all electronic votes given by the voter – occurs even more rarely. The share of cancelled i-votes per election has been below 0.1 per cent.

Third, a non-negligible share of e-votes are cast from abroad (by voters permanently or temporarily residing abroad, as well as by voters who were travelling). The total number of Estonian voters permanently living abroad is more than 80,000. As shown in Table 1, the share of i-votes cast in a foreign country has been around 4–6 per cent since 2015. In the 2019 Riigikogu elections, 6.3 per cent (or more than 15,000 votes) of all electronic votes were cast abroad, from 143 different countries. In comparison, fewer than 1400 votes were cast at Estonian representations abroad and via mail in the same election. These numbers illustrate the potential of i-voting to facilitate electoral participation in the era of migration and business-, leisure- and study-related mobility. The benefits are especially notable for a small nation with a sizable diaspora but a limited network of embassies and consulates.

Fourth, i-voting statistics provide information about the extent and ways in which voters use available technologies. While the ID-card remains the authentication option preferred by the majority of voters, voter authentication by mobile-ID, first introduced in 2011, has become increasingly widespread. In the 2011 general elections, 1.9 per cent of i-voters used mobile-ID order to authenticate themselves. In 2019, 30.1 per cent did so.[4] This trend reflects the increase in the number of mobile-ID users in the general population (Pappel et al., 2017). Interest in vote verification, in contrast, has remained tepid. The option to verify whether one’s vote was recorded as cast was first offered in the 2013 local elections. It was used by 3.4 per cent of i-voters. In subsequent elections, the share of i-voters who use the vote verification option has been consistently about 4 per cent, rising to 5.3 per cent in the 2019 Riigikogu election (see Table 1).

[4] https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

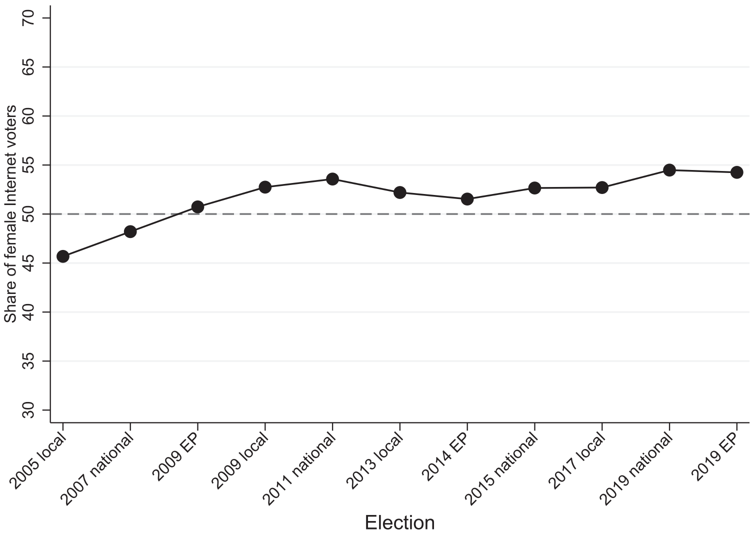

Fig. 4. Share of women among Internet voters 2005–2019 (Source: State Electoral Office).

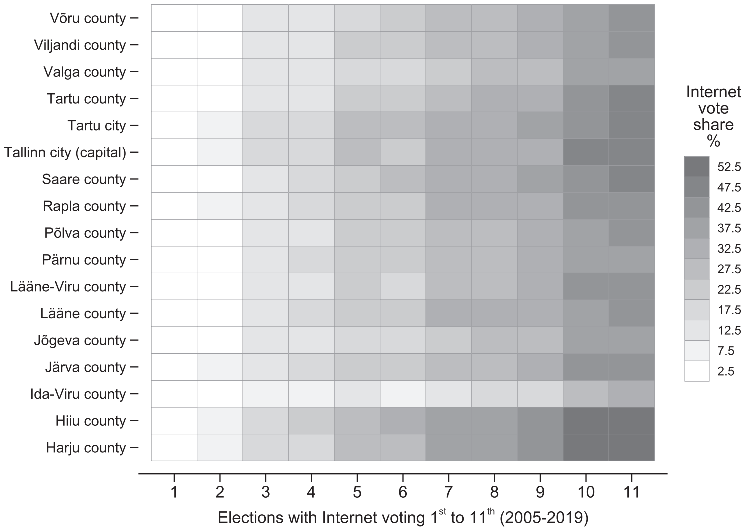

Fig. 5. Spread of Internet voting usage across Estonian regions (2005–2019) (Data source: State Electoral Office).

5.2. *User profiles*

Usage statistics cited above show an almost linear uptake of the technology as measured by the share of i-votes cast. Prior research has demonstrated that diffusion – defined as uptake of Internet voting by a demographically heterogeneous population – is non-linear and accelerates after a certain latency period during which usage spreads slowly in smaller tech-literate early adopter groups (Vassil et al., 2016). The same subtle change in the socio-demografic profiles of Internet voters is evident in the data below. Fig. 3 shows how the median age of the i-voter has gradually increased across elections and how the age structure of paper voters and i-voters has become more similar over time.

A comparable gradual change is evident in data on i-voters' gender. In Estonia, women have a higher propensity to vote than men. However, 54 per cent of i-votes cast in the very first i-vote enabled election in 2005 were given by men. This proportion started to reverse itself relatively quickly and is now the exact opposite, with female voters making up 54 per cent of i-voters in the 2019 elections as shown in Fig. 4.

The gradual diffusion of i-voting is evident from the changing effects of a number of other socio-demographic predictors. In the first i-elections, i-voters tended to be younger, male, highly educated, living in cities and earning higher incomes. This pattern no longer holds: the typical Internet voter in Estonia is a middle-aged, more likely female, mid-income voter (Vassil et al., 2016).

An analysis of regional dynamics suggest that the usage of Internet voting has gradually increased across all regions of the country. Fig. 5 shows the share of i-votes out of all votes cast in each of the 15 counties, the capital Tallinn, and the second-largest city Tartu, across all elections held 2005–2019. Harju county, which surrounds the capital, and Hiiu county, which is an island county with low population density, stand out with i-voting rates above the national average. Ida-Viru county, where a high share of the residents are members of Estonia's Russian-speaking minority, has the lowest prevalence of i-voting. Usage in other regions of the country is quite evenly spread.

The even spread of Internet voting across socio-demographic voter groups and geographical regions raises the question of what predicts usage when voter demographics no longer do?

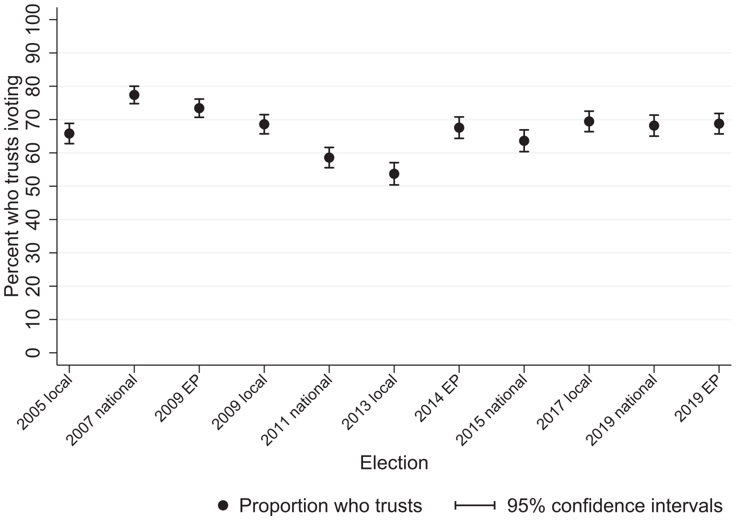

Fig. 6. Share of eligible voters who trust Internet voting (2005–2019) (Source: Estonian Internet voter study 2005–2019).

Table 2
Factors affecting Internet voting usage (2005–2019).

	2005 local	2007 national	2009 EP	2009 local	2011 national	2013 local	2014 EP	2015 national	2017 local	2019 national	2019 EP
Trust i-voting	0.51***	0.49***	0.41***	0.53***	0.35***	0.29***	0.17*	0.31***	0.42***	0.35***	0.41***
	(0.05)	(0.08)	(0.07)	(0.08)	(0.05)	(0.05)	(0.08)	(0.05)	(0.06)	(0.05)	(0.04)
Average trust of	0.02	0.11	– 0.03	– 0.03	– 0.15	– 0.01	0.16*	– 0.00	– 0.01	0.10	– 0.05
institutions	(0.05)	(0.07)	(0.05)	(0.06)	(0.08)	(0.06)	(0.07)	(0.05)	(0.06)	(0.06)	(0.07)
Trust of Internet	0.06	0.16	0.17*	– 0.03	0.04	– 0.08	– 0.06	0.07	– 0.04	0.07	– 0.05
transactions	(0.08)	(0.09)	(0.07)	(0.09)	(0.04)	(0.06)	(0.07)	(0.06)	(0.08)	(0.07)	(0.08)
Average PC lit.	0.02	0.07	– 0.02	– 0.04	0.04	0.11	– 0.02	– 0.05	0.17	0.04	0.10
(ref:poor/basic)	(0.09)	(0.09)	(0.06)	(0.08)	(0.08)	(0.07)	(0.09)	(0.07)	(0.11)	(0.12)	(0.10)
Good/v. good PC lit.	0.16	0.19*	– 0.01	0.08	0.05	0.10	0.17	0.06	0.30*	0.15	0.27**
(ref:poor/basic)	(0.09)	(0.09)	(0.06)	(0.084)	(0.08)	(0.09)	(0.07)	(0.11)	(0.12)	(0.12)	(0.10)
Internet usage	0.01	0.03*	0.01*	0.02	0.02	0.03*	0.04**	0.05***	0.03	0.02	0.01
frequency	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)	(0.02)	(0.01)
Age^2	0.00*	0.00**	0.00	– 0.00	– 0.00	– 0.00	0.00	0.00***	– 0.00	0.00	– 0.00
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.01)	(0.00)	(0.00)
Male	– 0.04	– 0.01	0.05	0.04	0.09*	0.02	– 0.01	0.09**	0.08*	– 0.05	0.17***
	(0.04)	(0.04)	(0.03)	(0.04)	(0.04)	(0.04)	(0.05)	(0.03)	(0.04)	(0.04)	(0.04)
Income decile	– 0.01	0.01	0.01	0.01	0.03**	0.00	0.01	0.00	– 0.00	0.01	– 0.00
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
Estonian	0.28***	0.42***	0.35***	0.32**	– 0.07	0.16**	– 0.07	0.03	0.25***	0.16**	0.08
	(0.06)	(0.09)	(0.07)	(0.06)	(0.07)	(0.05)	(0.06)	(0.05)	(0.11)	(0.06)	(0.08)
Secondary educ.	0.02	0.06	– 0.02	– 0.17	– 0.23*	0.11	– 0.05	– 0.02	0.17	– 0.016	0.09
(ref:basic)	(0.12)	(0.15)	(0.15)	(0.13)	(0.10)	(0.07)	(0.08)	(0.06)	(0.10)	(0.12)	(0.12)
Higher educ.	0.07	0.09	0.08	– 0.04	– 0.08	0.25**	0.00	0.03	0.25*	0.07	0.12
	(0.13)	(0.15)	(0.15)	(0.13)	(0.10)	(0.07)	(0.09)	(0.07)	(0.11)	(0.12)	(0.11)
Sensitivity	93.81	93.31	99.59	90.00	87.74	56.80	46.34	50.69	80.08	83.33	85.92
Specificity	51.19	44.00	44.85	53.01	56.94	87.25	88.36	89.30	62.54	61.96	57.22
Pseudo R^2	0.38	0.31	0.39	0.38	0.437	0.424	0.33	0.35	0.38	0.35	0.33
Observations	459	529	488	436	405	470	314	527	547	552	478

NOTE: Average marginal effects with standard errors in parentheses. *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$.

5.3. *Trust in i-voting: a persistent predictor of usage*

Aside from socio-demographic characteristics, individuals' beliefs and attitudes, computer skills, as well as access to technological infrastructures have been shown to influence the use of technologies. Specifically, trust has been identified as a major precondition for technology adoption and use (Lippert & Davis, 2006; McKnight et al., 2011; Vinkel, 2015).

To gauge voter trust in i-voting, we use individual-level survey data from the Estonian Internet voter study 2005–2019 (Johan, 2019), which covers all 11 elections in which i-voting has been available. Each post-election survey had a sample of roughly 1000 eligible voters; the combined dataset consists of 11,059 interviews. For information on sampling and interview methods, see Appendix A. Fig. 6 shows the dynamics of trust towards Internet voting. While there are some fluctuations across time and the type of election, the share of voters who trust i-voting hovers around 70 per cent.

To quantify the effects of trust, skills, Internet usage and voter demographics on the choice of voting mode, we estimate 11 logit regressions models, one for each election. Only self-reported voters are included in the analysis. The dependent variable is whether the respondent cast a paper ballot or an electronic one. Independent variables include trust in Internet voting, averaged trust in state institutions (government, parliament, parties, president and courts), trust in Internet transactions in general, self-reported personal computer (PC) skill level and Internet usage frequency measured as the number days per week the respondent uses the web. The models also include age, gender, income, ethnicity (Estonian or Russian-speaking), and education.

The results are shown in Table 2. Interestingly, the only variable that has consistently strong effects across the eleven elections is trust in Internet voting. In 2005 for example, the average marginal effect of trusting Internet voting was 0.51 which means that voters who trust i-voting have a 51 per cent higher likelihood of casting a ballot over the Internet as opposed to a paper vote, compared to those who do not trust i-voting. While the size of this effect fluctuates between 17 to 53 per cent depending on the election, the effect persists across all elections. Trust in state institutions or in Internet transactions in general, PC skills, and the frequency of using the Internet do not consistently differentiate between Internet and paper voters. Socio-demographic characteristics, with the partial exception of ethnicity, have weak and inconsistent effects when trust is controlled for. In sum, trust in i-voting is the key factor explaining usage even after the wide diffusion of this voting mode in the population.

6. I-voting and partisan politics

An analysis of the adoption and usage of Internet voting must take into account the role played by political parties. Parties are important players because they take decisions on the introduction and/or discontinuation of Internet voting, and they send signals to voters that either encourage or discourage the use of this voting mode. When it comes to collective choices about permissible voting modes, political parties have “skin in the game.” Because parties are interested in votes, they consider the implications of introducing or extending novel voting modes – postal, Internet or other – for their own and their opponents’ electoral fortunes. Party rhetoric for or against a particular voting mode can influence the behavior of voters – as exemplified by the results of the 2020 presidential election in the United States (Peeples, 2020).

Despite a sustained political commitment to developing i-voting that spans two decades and ten coalition governments, Internet voting in Estonia has been politically contested. Out of a total of ten parties that have held parliamentary seats since the early 2000s, two centre-right parties (Pro Patria and Reform Party) can be regarded as the main drivers and promoters of i-voting, while three – the Centre Party, the People’s Union, and its successor, the Conservative People’s Party – have adopted critical stances at various points of time. The Centre Party is a large centre-left party with a populist streak. The People’s Union was associated, above all, with rural interests, while the Conservative People’s Party is classified as populist far-right (Rooduijn et al., 2019).

Both the Centre Party and the People’s Union voted against the introduction of i-voting in the 2005 local elections. Former Chairman of the People’s Union, Arnold Rüütel, then President of the Republic, twice refused to proclaim the law instituting Internet voting, arguing that the possibility to cast multiple electronic votes violates the principle of uniformity of elections (see Section 4.2). The Centre Party stepped up criticism of Internet voting prior to October 2013 local elections. In spring 2013, an NGO connected to the Centre Party ran a street campaign in Tallinn, featuring posters with slogans such as “They may delete your vote”, “Every i-vote is a potential threat to Estonia’s independence” and “They can give your vote to whoever they want” (Velsker & Olup, 2017). In October 2013, the Centre-controlled Tallinn city government organized a public forum entitled “The Devil elects over the Internet” (Kossar, 2015) and funded the visit of foreign experts who produced a highly critical report of the Estonian i-voting system (Springall et al., 2014). After the election, Centre Party Chairman Edgar Savisaar claimed that centre-right parties won the election by forging election results (Velsker & Olup, 2017). In 2014, the Centre Party board sent a letter to Estonian and EU top officials requesting immediate cancellation of Internet voting due to “fundamental security problems” (Villmann, 2014). In April 2015, the Party’s Council adopted a resolution which claimed that online voting is a security risk, and argued that i-voting violates the requirements of uniformity and secrecy (Keskerakond, 2015).

However, the Centre Party mostly discontinued its criticism of Internet voting after it became the leading government party in November 2016. In September 2017, the government led by Jüri Ratas had to manage the most serious crisis in the history of Estonian e-government which occurred after foreign scientists found a vulnerability affecting hundreds of thousands of Estonian ID-cards (see Section 4.1). With the reputation of Estonian e-government system at stake, the government led by Ratas worked hard to solve the crisis and control damage. Since the event, the Centre Party has not voiced any significant criticism of Internet voting. In fact, the government led by Ratas actively encouraged the voters to vote over the Internet in the October 2017 local elections.

Founded in 2012, the Estonian Conservative People’s Party (EKRE) first gained parliamentary representation in 2015 and was part of the Centre-led governing coalition from April 2019 to January 2021. While the party kept a low profile on Internet voting during the first four years of its existence, it has, over time, turned into a vocal critic of the system, questioning its integrity and calling for international audits and the cancellation of i-voting. In June 2019, an EKRE minister convened an expert group tasked with assessing the integrity and security of the i-voting system. The group, however, did not find any reasons to discontinue or limit i-voting. Its final report, published in December 2019, lists 25 recommendations for improving the system, topped by a call to ensure “sufficient and sustainable funding” for maintaining and developing the system and the need to improve “understanding” of the system among observers and the general public (E-valimiste turvalisuse töörühm, 2019).

Data from the Estonian Internet voter study 2005–2019 suggests that voters’ trust in i-voting varies according to the position of the voters’ preferred party. In other words, Centre Party and EKRE voters are significantly less likely to trust i-voting than voters who supported parties that have consistently endorsed i-voting. Based on a survey conducted after the 2019 Riigikogu elections, the share of those who trust i-voting was between 40 and 50 per cent among Centre Party and EKRE voters, while among the supporters of other parliamentary parties, the share of trusters exceeded 80 per cent (Johan, 2019). These preliminary results illustrate the potential of parties to shape the attitudes of voters; a more careful analysis of cue-giving and cue-taking remains a task for a separate study. In this context, it is important to note that academic studies on the political neutrality of Internet voting have not identified any bias-inducing mechanisms – such as non-random voter mobilization, vote switching and mode specific bias – in the Estonian case (Solvak & Vassil, 2016, pp. 142–162).

In sum, the fact that parties opposed to i-voting have been in opposition or in the role of a junior coalition partners for most of the past 20 years is central to explaining the adoption and expansion of Internet voting in Estonia. By the time the Centre Party secured a prime ministerial position (November 2016) and the Estonian Conservative People’s Party joined the Centre-led government (April 2019), i-voting had become effectively entrenched: the system was used across the socio-demographic board, enjoyed high levels of trust among the electorate, and had become part of the internationally promoted e-Estonia success story. The fall of the Centre-led government in January 2021, followed by the formation of a new government led by the liberal, pro-market Reform Party, signifies a return to the previous norm of strong governmental support to i-voting in Estonia.

7. Conclusions and discussion

Over the past two decades, enthusiasm for Internet voting around the world appears to have gone from boom to bust, as high hopes of the early 2000s have given way to concerns about technological failures and election hacking, along with the widespread belief that Internet voting is incapable of delivering transparency, verifiability and privacy simultaneously. However, it is likely that there will be a new surge of interest in Internet voting, driven by technological advances, progressive digitalization of societies, growing mobility of individuals, as well as specific triggers such as the global pandemic. In this context, the Estonian experience with Internet voting offers unique insights into possible electoral futures.

The main finding of this article is that over a period of fifteen years, Internet voting has become normalized and even entrenched in Estonia. Electoral authorities no longer regard it as an experiment: i-voting is an essential part of the regular framework for conducting elections. High usage rates and strong trust among the electorate suggest that the majority of citizens share this assessment, increasingly regarding i-voting as a routine practice. The practice has been upheld by the courts and accepted by international organizations monitoring elections and democracy.

Why did Estonia continue to develop Internet voting while many other countries and communities discontinued the practice after limited pilots? This analysis suggests that Estonia's diverging trajectory is the result of several factors. First, timing matters – as a pioneer in the field, Estonia had put the i-voting system in place before cyber-attacks, election hacking and malign interventions became commonplace. This means that in the critical phase of adoption and early development, there were fewer fears and hence, less opposition. Second, in Estonia, the introduction and development of Internet voting has been a part of a broader concerted effort to build a digital state. The Estonian i-voting system differs from systems used in other countries in that it is based on a highly developed national electronic identification scheme that is the cornerstone of the Estonian e-state. Secure state-issued digital identities are used widely in citizens' daily transactions in the public and private sectors. The resulting normalization and routinization of digital transactions has greatly facilitated the uptake and diffusion of Internet voting. Third, the system has performed without major glitches and has become highly popular. With almost half of all votes cast over the Internet, it is difficult for any political actor to advocate discontinuation. Fourth, i-voting in Estonia has enjoyed persisting political support. While there have been periods marked by significant partisan conflict over Internet voting, party-based opposition has gradually waned as i-voting has spread across socio-demographic groups and as parties have taken turns in shouldering the responsibilities of government. Fifth, the government and electoral authorities have been committed to improving, developing and updating the technological, legal and organizational aspects of the i-voting system and have put great effort into anticipating and mitigating risks. Finally, the fact that i-voting is regarded as an integral element of the widely acclaimed Estonian digital state and society means that a range of domestic actors are deeply vested in the continued performance of the system. The political and reputational costs of abandoning i-voting would be very high, extending far beyond the realm of election administration.

We offer five main takeaways from our analysis. First, Estonia's exceptionalism in the realm of Internet voting must be understood in the context of particular enabling conditions such as the existence of an advanced national digital infrastructure and strong digital identities bestowed on all residents. In a context where all citizens have access to secure digital authentication and digital signatures and the vast majority use these functionalities on a regular basis, there is no need to develop authentication solutions specifically for elections. The key reason why people trust and use i-voting in Estonia is that it is embedded in a broader system of e-governance that works, as confirmed by residents' everyday experiences. The Estonian experience suggests that governments that seek to deploy Internet voting on a large scale should start by conferring strong digital identities upon their citizens. Developing secure electronic authentication systems is a priority for governments around the world. In Europe, the European Commission has defined minimum technical specifications and procedures for assurance levels for electronic identification, and the European Union's eIDAS (Electronic Identification, Authentication and Trust Services) regulation, adopted in 2014, lays down the conditions under which member states recognize each others' national electronic identification schemes (The European Parliament and the Council of the European Union, 2014). The existence of EU-wide standards has the potential to build trust and encourage the uptake and use of electronic IDs by member state citizens. Once digital authentication is routinely used in a variety of online transactions, citizens are likely to become increasingly open to the idea of casting votes via the Internet.

The second takeaway is that Internet voting complicates election administration instead of simplifying it. By deploying i-voting, governments take on a long-term obligation to develop technology, build legal frameworks, adjust election administration, and defend the system against attacks, criticism, and disinformation on both the domestic and the international arena. Developing a regulatory framework for i-voting takes time, entails significant normative innovation, and requires persistent efforts to explain and defend the system vis-a-vis established standards for democratic elections. While large-scale i-voting can reduce the need to deploy and staff polling stations, the challenge of deploying i-voting and administering it in parallel with the conventional paper-based voting system should not be underestimated. In sum, the Estonian experience suggests that large-scale deployment of i-voting increases administrative complexity and augments the workload of electoral authorities. This means that countries with significant election administration problems and understaffed or underfunded electoral authorities should refrain from deploying remote Internet voting on a large scale. Online voting should be seen as an advanced service, as opposed to a quick fix to existing problems. Developing countries, countries undergoing regime transitions, as well as federal countries with complicated multi-level jurisdictions should carefully assess potential risks and difficulties before deciding to introduce i-voting.

The third conclusion is that the deployment of Internet voting does not increase electoral participation – at least not in countries where access to voting is already very good and where early voting is widely available. Aggregate data from eleven Estonian elections shows that despite massive uptake of i-voting, rates of electoral participation have remained stable. This, combined with the finding from previous studies that the uptake of i-voting is lowest among those segments of the Estonian electorate that are least likely to vote, suggests that Internet voting facilitates electoral participation for those who intended to vote anyway. It does not motivate non-voters to take part in elections. Thus, in settings where voting is already easily accessible, i-voting is primarily about voter convenience and choice, i.e. about providing a better service to the electorate. This means that countries should not base the decision to deploy remote Internet voting on expectations of increased turnout, including among young voters – with the possible exception of countries where long distances, poor infrastructure or difficult terrain hinder access to physical voting locations. Because i-voting allows citizens to cast votes from anywhere in the world, Internet voting has the potential to increase turnout in countries with sizable diaspora or expatriate communities.

The fourth takeaway is that Internet voting should not be automatically associated with digital divides and differential opportunities for different socioeconomic groups. In Estonia, i-voting has diffused to the extent that age, education, gender and income no longer predict usage. While there are some regional differences, these are not pronounced: i-voting is widely used in cities and in rural areas, in the capital and in the periphery. The broader lesson here is that uptake and diffusion are central to the long-term sustainability of i-voting: the question of user demographics is central to political parties' reasoning about the electoral effects of Internet voting, and hence, their propensity to support or oppose the deployment of i-voting. In any case, the diffusion of Internet voting takes time, and political decision-makers are advised to be patient in drawing conclusions about the success and effects of the novel voting mode.

The fifth and final conclusion reiterates the importance of trust as a precondition for the adoption and use of new technologies. Our data showed that in Estonia, trust in Internet voting is the single most important predictor of casting an electronic ballot as opposed to a paper one. While analyzing the complex process of how trusting attitudes are formed and maintained was beyond the scope of this study, our analysis points to an understanding of trust that is deeply contextual. Trust is not just a reflection of the features of specific technologies such as an Internet voting application – instead, it emerges from the normalization, institutionalization and routinization of particular practices in the context of broader socio-technological systems. Introducing i-voting in a low-trust environment is likely to do more harm than good. This realization suggests that without a deep and systemic digital transformation that enables and habitualizes the use of secure digital identities and allows citizens to build confidence in the digital capabilities of the state and society, Internet voting is unlikely to develop beyond the experimental stage of small-scale pilots. Thus, paraphrasing timeless advice from the Cheshire cat: in the wonderland of Internet voting, where one ought to start depends a good deal on where one wants to get to.

Funding

This work was supported by the Horizon 2020 Framework Programme grant number 857622 and the Estonian Research Council grant number PRG920. The financing agencies and authors' employers had no role in study design; in the collection, analysis and interpretation of data; in the writing of the report; and in the decision to submit the article for publication.

Declaration of Competing Interest

Priit Vinkel was engaged in Estonian election management from 2005 until 2019, serving as the Head of the State Electoral Office from 2013 to 2019. Since 2020, he is a part-time researcher at Cybernetica, the company that developed the Estonian Internet voting solution.

Since 1998, Jan Willemson has worked as a researcher at Cybernetica, the company that developed the Estonian Internet voting solution.

Appendix A. Survey descriptions and trust measurement

All surveys are post-election surveys with fieldwork conducted over 30 days after the election date. The 2005–2011 surveys used quota sampling according to voting mode due to the still relatively low number of i-voters in the population. The samples are representative for eligible voters in terms of age, gender, ethnicity and region. The 2013 to 2019 surveys used stratified random samples and are representative for eligible voters in terms of age, gender, ethnicity, settlement type and region. Table 3 lists the interview methods and number of respondents for all the surveys used in this study.

The key variable of interest – trust in i-voting – was measured with the question: "Do you trust Internet voting?". From 2005 to 2011, the answers were recorded on a four-category Likert scale, while between 2013–2019, a 0–10 scale was used. To produce results that can be compared across years (Fig. 6), both the Likert scale and the 0–10 scale were split in the middle, with respondents on scale point 5 randomly assigned to either side.

Table 3
Description of post-election surveys used in the study.

Post-election survey	Sampling method	Interview method	Number of respondents
2005 local	quota sample (1/3 non-voters; 1/3 paper voters; 1/3 e-voters)	CATI	1000
2007 national	quota sample (1/3 non-voters; 1/3 paper voters; 1/3 e-voters)	CATI	1000
2009 EP	quota sample (1/3 non-voters; 1/3 paper voters; 1/3 e-voters)	CATI	1000
2009 local	quota sample (1/3 non-voters; 1/3 paper voters; 1/3 e-voters)	CATI	1000
2011 parliamentary	quota sample (1/3 non-voters; 1/3 paper voters; 1/3 e-voters)	CATI	1007
2013 local	stratified random sample	CAPI	1042
2014 EP	stratified random sample	CAPI	1001
2015 parliamentary	stratified random sample	CAPI	1007
2017 local	stratified random sample	CATI	1000
2019 parliamentary	stratified random sample	CATI	1000
2019 EP	stratified random sample	CATI	1002

References

Alvarez, R. M., & Hall, T. E. (2004). *Point click, and vote: The future of internet voting.* Brookings Institution Press.

Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009). Internet voting in comparative perspective: The case of Estonia. *PS: Political Science and Politics, 42*, 497–505. https://doi.org/10.1017/S1049096509090787

Ansper, A., Buldas, A., Jürgenson, A., Oruaas, M., Priisalu, J., Raiend, K., Veldre, A., Willemson, J., & Virunurm, K. (2003). *E-voting concept security: Analysis and measures Report number EH-02-02, updated and translated to English in 2010*. https://www.valimised.ee/sites/default/files/uploads/eng/E-voting_concept_security_analysis_and_measures_2010.pdf.

Appel, A. W., Ginsburg, M., Hursti, H., Kernighan, B. W., Richards, C. D., & Tan, G. (2008). *Insecurities and inaccuracies of the Sequoia AVC advantage 9.00 H DRE voting machine*.

Appel, A. W., Ginsburg, M., Hursti, H., Kernighan, B. W., Richards, C. D., Tan, G., & Venetis, P. (2009). *The New Jersey voting-machine Lawsuit and the AVC advantage DRE voting machine 2009 electronic voting technology workshop /workshop on trustworthy elections EVT/WOTE'09 USENIX. association*.

Applegate, M., Chanussot, T., & Blasysty, V. (2020). *Considerations on internet voting: An overview for electoral decision-makers*. https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf.

Aviv, A. J., Cerný, P., Clark, S., Cronin, E., Shah, G., Sherr, M., & Blaze, M. (2008). Security evaluation of ES &S voting machines and election management system. In *2008 USENIX/ACCURATE electronic voting workshop*. EVT.

Bannet, J., Price, D. W., Rudys, A., Singer, J., & Wallach, D. S. (2004). Hack-a-vote: Security issues with electronic voting systems. *IEEE Security & Privacy, 2*, 32–37. https://doi.org/10.1109/MSECP.2004.1264851

BBC. (2014). *E-voting experiments end in Norway amid security fears BBC*. https://www.bbc.com/news/technology-28055678.

Binder, N. B., Krimmer, R., Wenda, G., & Fischer, D. H. (2019). International standards and ICT projects in public administration: Introducing electronic voting in Norway, Estonia and Switzerland compared. *Administrative Culture, 19*, 8–21. https://doi.org/10.32994/hk.v19i2.215

Bull, C., Gjosteen, K., & Nore, H. (2018). Faults in Norwegian internet voting. In *Proceedings of E-Vote-ID 2018* (pp. 166–169). TUT Press.

Council of Europe. (2004). *Recommendation CM/Rec(2004)11 on legal, operational and technical standards for e-voting*. https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf.

Council of Europe. (2011). *Guidelines on transparency of e-enabled elections*. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?.documentId=090000168059bdf6.

Council of Europe. (2017). *Recommendation CM/Rec(2017)5 of the committee of ministers to member states on standards for e-voting*. https://search.coe.int/cm/Pages/result_details.aspx?.ObjectID=0900001680726f6f.

Culnane, C., Essex, A., Lewis, S. J., Pereira, O., & Teague, V. (2019). Knights and knaves run elections: Internet voting and undetectable electoral fraud. *IEEE Security & Privacy, 17*, 62–70. https://doi.org/10.1109/MSEC.2019.2915398

Dill, D. L., Schneier, B., & Simons, B. (2003). Voting and technology: Who gets to count your vote? *Communication ACM, 46*, 29–31. https://doi.org/10.1145/859670.859692

Duenas-Cid, D., Krivonosova, I., Serrano, R., Freire, M., & Krimmer, R. (2020). Tripped at the finishing line: The Åland Islands internet voting project. In R. Krimmer, M. Volkamer, B. Beckert, R. Küsters, O. Kulyk, D. Duenas-Cid, & M. Solvak (Eds.), *Electronic voting* (pp. 36–49). Cham: Springer International Publishing.

E-valimiste turvalisuse töörühm. (2019). *E-valimiste turvalisuse töörühma koondaruanne*. https://www.mkm.ee/sites/default/files/e-valimiste_tooruhma_koondaruanne_12.12.2019.pdf.

Estonian Police, & Border Guard Board. (2017). *Estonia resolves its ID-card crisis* (p. 2017). https://www2.politsei.ee/en/uudised/uudis.dot?.id=801245.

European Commission. (2020). *eGovernment benchmark 2020: eGovernment that works for the people*. https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2020-egovernment-works-people.

Farzaliyev, V., Krips, K., & Willemson, J. (2021). Developing a personal voting machine for the Estonian internet voting system. In *Proceedings of the The 36th ACM/SIGAPP Symposium On Applied Computing* (pp. 1607–1616). ACM. https://doi.org/10.1145/3412841 3442034.

Federal Chancellery of the Swiss Confederacy. (2021). *Official infopage of the Swiss E-voting solution*. https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html.

Feldman, A. J., Halderman, J. A., & Felten, E. W. (2007). Security analysis of the diebold accuvote-TS voting machine. In *2007 usenix/accurate electronic voting technology workshop*. EVT.

Finnish Ministry of Justice. (2017). *Prerequisites for using internet voting in finland. A feasibility study*. https://julkaisut.valtioneuvosto.fi/handle/10024/160412.

Freedom House. (2020). *Freedom in the world: Estonia country report 2020*. https://freedomhouse.org/country/estonia/freedom-world/2020.

Germann, M. (2021). Internet voting increases expatriate voter turnout. *Government Information Quarterly, 38*(2). https://doi.org/10.1016/j.giq.2020.101560

Germann, M., & Serdült, U. (2017). Internet voting and turnout: Evidence from Switzerland. *Electoral Studies, 47*, 1–12. https://doi.org/10.1016/j.electstud.2017.03.001

Gerring, J. (2008). Case selection for case-study analysis: Qualitative and quantitative techniques. In J. M. Box-Steffensmeier, H. E. Brady, & D. Collier (Eds.), *The Oxford handbook of political methodology* (pp. 645–684). Oxford: Oxford University Press.

Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of e-voting: The past, present and future. *Annals of Telecommunications, 71*, 279–286. https://doi.org/10.1007/s12243-016-0525-8

Goodman, N., & Gabel, C. (2020). Internet voting: Strengthening Canadian democracy or weakening it? *Digital Politics in Canada: Promises and Realities*, 90–111.

Heiberg, S., Laud, P., & Willemson, J. (2011). The application of I-voting for Estonian parliamentary elections of 2011. In A. Kiayias, & H. Lipmaa (Eds.), *E-Voting and Identity – Third international conference, voteid 2011, Tallinn, Estonia, revised selected papers* (pp. 208–223). Cham: Springer.

Heiberg, S., Martens, T., Vinkel, P., & Willemson, J. (2016). Improving the verifiability of the Estonian internet voting scheme. In R. Krimmer, M. Volkamer, J. Barrat, J. Benaloh, N. J. Goodman, P. Y. A. Ryan, & V. Teague (Eds.), *Electronic Voting – First international joint conference, E-vote-id 2016, Bregenz, Austria, proceedings* (pp. 92–107). Cham: Springer.

Heiberg, S., Parsovs, A., & Willemson, J. (2015). Log Analysis of Estonian Internet Voting 2013-2014. In R. Haenni, R. E. Koenig, & D. Wikström (Eds.), *E-Voting and Identity – 5th international conference, voteid 2015, Bern, Switzerland proceedings* (pp. 19–34). Cham: Springer.

Heiberg, S., & Willemson, J. (2014a). Modeling threats of a voting method, in: Design, development, and Use of secure electronic voting systems. *IGI Global*, 128–148. https://doi.org/10.4018/978-1-4666-5820-2.ch007

Heiberg, S., & Willemson, J. (2014b). Verifiable internet voting in Estonia. In R. Krimmer, & M. Volkamer (Eds.), *6th International conference on electronic voting: Verifying the vote, evote 2014, Lochau /Bregenz, Austria* (pp. 1–8). IEEE. https://doi.org/10.1109/EVOTE.2014.7001135.

Heinmaa, A. E. (2020). *Special voting arrangements (SVAs) in Europe: In-country postal, early, mobile and proxy arrangements in individual countries*. https://www.idea.int/news-media/news/special-voting-arrangements-svas-europe-country-postal-early-mobile-and-proxy.

International Institute for Democracy, & Electoral Assistance. (2021). *Global overview of COVID-19: Impact on elections*. https://www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections.

IVTF. (2018). *Findings and asessment report of internet voting task force on voting rights of overseas Pakistanis*.

Jafar, U., & Ab Aziz, M. J. (2020). A state of the art survey and research directions on blockchain based electronic voting system. In *International conference on advances in cyber security* (pp. 248–266). Springer. https://doi.org/10.1007/978-981-33-6835-4_17.

Johan. (2019). *Skytte institute of political studies tartu university, 2021. Estonian Internet voter study 2005- Data available depending on request: mihkel.solvak@ut.ee*.

Kalja, A., Reitsakas, A., & Saard, N. (2005). *eGovernment in Estonia: Best practices, in: A unifying discipline for melting the boundaries technology management* (pp. 500–506). https://doi.org/10.1109/PICMET.2005.1509730

Keskerakond. (2015). *E-riigis on suurepärane kõik peale e-valimiste*. https://www.keskerakond.ee/et/530-keskerakonna-volikogu-avaldus-e-riigis-on-suurepaerane-koik-peale-e-valimiste.

Kossar, K. (2015). *Savisaar avab foorumi Saatan valib internetis postimees*. https://www.postimees.ee/2328366/savisaar-avab-foorumi-saatan-valib-internetis.

Krimmer, R. (2012). *The evolution of e-voting: Why voting technology is used and how it affects democracy*. Tallinn: Tallinn University of Technology. Ph.D. thesis.

Krimmer, R., Duenas-Cid, D., & Krivonosova, I. (2021a). Debate: Safeguarding democracy during pandemics. Social distancing, postal, or internet voting-the good, the bad or the ugly? *Public Money & Management, 41*, 8–10. https://doi.org/10.1080/09540962.2020.1766222

Krimmer, R., Duenas-Cid, D., & Krivonosova, I. (2021b). New methodology for calculating cost-efficiency of different ways of voting: Is internet voting cheaper? *Public Money & Management, 41*, 17–26. https://doi.org/10.1080/09540962.2020.1732027

Krimmer, R., Duenas-Cid, D., Krivonosova, I., Serrano, R. A., Freire, M., & Wrede, C. (2019). *Nordic pioneers: Facing the first use of internet voting in the AAland Islands (parliamentary elections 2019)*. https://doi.org/10.31235/osf.io/5zr2e

Krimmer, R., Triessnig, S., & Volkamer, M. (2007). The development of remote e-voting around the world: A review of roads and directions. In A. Alkassar, & M. Volkamer (Eds.), *E-voting and identity, first international conference, vote-id 2007, Bochum, Germany revised selected papers* (pp. 1–15). Berlin, Heidelberg: Springer. volume 4896 of Lecture Notes in Computer Science.

Krips, K., & Willemson, J. (2019). *On practical aspects of coercion-resistant remote voting systems* (pp. 216–232). Cham: International Joint Conference on Electronic Voting Springer.

Kuenzi, R. (2019). *These are the arguments that sank e-voting in Switzerland. SWI swissinfo.ch*. https://www.swissinfo.ch/eng/e-voting_these-are-the-arguments-that-sank-e-voting-in-switzerland/45136608.

Küsters, R., & Müller, J. (2017). *Cryptographic security analysis of e-voting systems: Achievements, misconceptions, and limitations, in: International joint conference on electronic voting* (pp. 21–41). Cham: Springer.

Lipmaa, H., & Mürk, O. (2001). *E-valimiste realiseerimisvoimaluste analüs*. https://www.valimised.ee/sites/default/files/uploads/eh/lipmaamyrk.pdf.

Lippert, S. K., & Davis, M. (2006). A conceptual model integrating trust into planned change activities to enhance technology adoption behavior. *Journal of Information Science, 32*, 434–448. https://doi.org/10.1177/0165551506066042

LRT English. (2020). *Lithuanian government backs online voting, but with caveats*. https://www.lrt.lt/en/news-in-english/19/1190786/lithuanian-government-backs-online-voting-but-with-caveats.

Marky, K., Kulyk, O., & Volkamer, M. (2018). Comparative usability evaluation of cast-as-intended verification approaches in internet voting. *SICHERHEIT*. https://doi.org/10.18420/sicherheit2018_15

Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society, 3*, 213–233. https://doi.org/10.1007/s12394-010-0044-0

McBrien, T. (2020). Defending the vote: Estonia creates a network to combat disinformation. *Series: Innovations for Successful Societies*.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems, 2*, 1–25. https://doi.org/10.1145/1985347.1985353

Nemec, M., Sýs, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The return of coppersmith's attack: Practical factorization of widely used RSA moduli. In B. M. Thuraisingham, D. Evans, T. Malkin, & D. Xu (Eds.), *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, CCS 2017, Dallas, TX, USA* (pp. 1631–1648). https://doi.org/10.1145/3133956.3133969

NSW Electoral Commission. (2020). *iVote online and telephone voting*. https://www.elections.nsw.gov.au/Voters/Other-voting-options/iVote-online-and-telephone-voting.

OECD. (2020). *OECD broadband statistics update*. http://www.oecd.org/digital/broadband-statistics-update.htm.

OSCE/ODIHR. (2007). *OSCE/ODIHR election assessment mission report on parliamentary elections 4 March 2007*. https://www.osce.org/files/f/documents/1/1/25925.pdf.

OSCE/ODIHR. (2011). *OSCE/ODIHR election assessment mission report on parliamentary elections 6.03.2011*. https://www.osce.org/files/f/documents/a/9/77557.pdf.

OSCE/ODIHR. (2015). *OSCE/ODIHR election expert team report on parliamentary elections 1.03.2015*. https://www.osce.org/files/f/documents/a/4/160131.pdf.

OSCE/ODIHR. (2019). *OSCE/ODIHR election expert team report on parliamentary elections 3.03.2019*. https://www.osce.org/files/f/documents/8/e/424229.pdf.

Pappel, I., Pappel, I., Tepandi, J., & Draheim, D. (2017). *Systematic digital signing in Estonian e-government processes, in: Transactions on large-scale data-and knowledge-centered systems XXXVI* (pp. 31–51). Berlin, Heidelberg: Springer.

Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: From internet voting to blockchain voting. *Journal of Cybersecurity, 7*, 1–15. https://doi.org/10.1093/cybsec/tyaa025

Parsovs, A. (2020). Solving the Estonian ID card crisis: The legal issues. In *ISCRAM 2020 conference proceedings-17th international conference on information systems for crisis response and management* (pp. 459–471). ISCRAM.

Parsovs, A. (2021). *Estonian electronic identity card and its security challenges*. Tartu: University of Tartu. https://dspace.ut.ee/handle/10062/71481.

Peeples, L. (2020). *COVID and the US election: Will the rise of mail-in voting affect the result?. Nature*. https://doi.org/10.1038/d41586-020-02979-x

Raag, T. (2020). *Eesti digiriik naudib NII kohalike elanike kui e-residentide toetust*. https://www.pealinn.ee/tallinn/eesti-digiriik-naudib-nii-kohalike-elanike-kui-e-residentide-toetust-n254601.

Reuters. (2017). *France drops electronic voting for citizens abroad over cybersecurity fears reuters 6*. https://www.reuters.com/article/us-france-election-cyber-idUSKBN16D233.

Riigikogu. (2015). *Explanatory memorandum to draft 160se in the estonian parliament*. https://www.riigikogu.ee/download/181c73f1-8840-40b4-b156-1277653b4eb1.

Rooduijn, Kessel, V., Froio, Pirro, Lange, D., Halikiopoulou, Lewis, Mudde, & Taggart. (2019). *The populist: An overview of populist, far right far left and eurosceptic parties in Europe*. https://popu-list.org.

Solvak, M., & Vassil, K. (2016). *E-voting in Estonia: Technological diffusion and other developments over ten years (2005–2015)*. Tartu: Johan Skytte Institute of Political Studies University of Tartu.

Solvak, M., & Vassil, K. (2018). Could internet voting halt declining electoral turnout?. new evidence that e-voting is habit forming. *Policy & Internet, 10*, 4–21. https://doi.org/10.1002/poi3.160

Specter, M., & Halderman, J. (2021). Security analysis of the democracy live online voting system. In *30th USENIX security symposium (USENIX Security 21) forthcoming*. https://www.usenix.org/system/files/sec21summer_specter-security.pdf.

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security analysis of the Estonian internet voting system. In *Proceedings of the 21st ACM conference on computer and communications security* (pp. 703–715). ACM. https://doi.org/10.1145/2660267.2660315.

Stake, R. E. (1995). *The art of case study research*. Thousand Oaks, CA 91320: Sage Publications, Inc.

State Electoral Office of Estonia. (2017). *General framework of electronic voting and implementation thereof at national elections in Estonia*. https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-10-eng.pdf.

State Information System Authority. (2020). *State information system authority yearbook 2020*. https://www.ria.ee/sites/default/files/content-editors/RIA/ria_aastaraamat_2020_48lk_est_veeb.pdf.

Statistics Estonia. (2021a). *Computer and internet users aged 16-74 by group of individuals*. http://andmebaas.stat.ee/Index.aspx.

Statistics Estonia. (2021b). *Households having a computer and internet connection at home by type of household and place of residence*. http://andmebaas.stat.ee/Index.aspx.

Supreme Court of Estonia. (2005). *Supreme court judgement 3-4-1-13-05 1.09.2005 on constitutionality of the Estonian internet voting system*. https://www.riigikohus.ee/en/constitutional-judgment-3-4-1-13-05.

Supreme Court of Estonia. (2011). *Supreme court judgement 3-4-1-4-11 21.03.2011 on a complaint to declare i-voting results invalid*. https://www.riigikohus.ee/et/lahendid?.asjaNr=3-4-1-4-11.

Supreme Court of Estonia. (2013). *Supreme Court judgement 3-4-1-57-13 19.11.2013 on a complaint to declare i-voting results invalid*. https://www.riigikohus.ee/et/lahendid?.asjaNr=3-4-1-57-13.

Supreme Court of Estonia. (2017). *Supreme court judgement 5-17-35 24.10.2017 on a complaint to declare i-voting results invalid*. https://www.riigikohus.ee/et/lahendid?.asjaNr=5-17-35/2.

Supreme Court of Estonia. (2019a). *Supreme court judgement 5-19-18 27.03.2019 on need for additional law-level regulations on i-voting*. https://www.riigikohus.ee/et/lahendid/?asjaNr=5-19-18/3.

Supreme Court of Estonia. (2019b). *Supreme court judgement 5-19-20 27.03.2019 on need for additional law-level regulations on i-voting*. https://www.riigikohus.ee/et/lahendid?asjaNr=5-19-20/2.

Tammet, T., & Krosing, H. (2001). *E-valimised eesti vabariigis: Voimaluste analus*. https://www.valimised.ee/sites/default/files/uploads/eh/evalimisteanalyys24okt.doc.

The European Parliament the Council of the European Union. (2014). *Regulation (EU) No 910/2014 of the European parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. https://eur-lex.europa.eu/legal-content/EN/TXT/?.uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

The Indian Express. (2015). *After compulsory voting, Gujarat now offers the online option. 20 february*. https://indianexpress.com/article/india/india-others/after-compulsory-voting-gujarat-now-offers-the-online-option/.

Trechsel, A. H., & Vassil, K. (2011). *Internet voting in Estonia: A comparative analysis of four elections since 2005 Report for the Council of Europe*. Strassbourg: Council of Europe.

United Nations. (2020). *United nations e-government survey 2020: Digital government in the decade of action for sustainable development*. https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey.

Vote Foundation, U. S. (2015). *The future of voting: End-to-end verifiable internet voting. Specification and feasibility assessment study*. https://www.usvotefoundation.org/E2E-VIV.

Vassil, K., Solvak, M., Vinkel, P., Trechsel, A. H., & Alvarez, R. M. (2016). The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Government of Information Quarterly, 33*, 453–459. https://doi.org/10.1016/j.giq.2016.06.007

Vassil, K., & Weber, T. (2011). A bottleneck model of e-voting: Why technology fails to boost turnout. *New media & society, 13*, 1336–1354. https://doi.org/10.1177/1461444811405807

Velsker, L., & Olup, N. M. (2017). ülevaade: Keskerakonna voitlused e-valimiste vastu. *Postimees*. https://www.postimees.ee/4233855/ulevaade-keskerakonna-voitlused-e-valimiste-vastu.

Villmann, A. L. (2014). *Keskerakond nouab Euroopa parlamendilt e-valimiste tühistamist*. ERR. https://www.err.ee/512935/keskerakond-nouab-euroopa-parlamendilt-e-valimiste-tuhistamist.

Vinkel, P. (2015). *Remote electronic voting in Estonia: Legality, impact and confidence*. Tallinn, Estonia: Tallinn University of Technology.

Willemson, J. (2018). Bits or paper: Which should get to carry your vote? *Journal Information Security Application, 38*, 124–131. https://doi.org/10.1016/j.jisa.2017.11.007

Wilson, A. (2019). Modeling requirements conflicts in secret ballot elections. In *Proceedings of E-Vote-ID 2019* (pp. 171–186). TalTech Press.

Wolchok, S., Wustrow, E., Halderman, J. A., Prasad, H. K., Kankipati, A., Sakhamuri, S. K., Yagati, V., & Gonggrijp, R. (2010). Security analysis of India's electronic voting machines. In *Proceedings of the 17th ACM CCS* (pp. 1–14). https://doi.org/10.1145/1866307.1866309

Yin, R. K. (2018). *Case study research and applications: Design and methods*. Thousand Oaks, CA 91320: Sage.

Piret Ehin is a Professor in Comparative Politics and Deputy Head of Johan Skytte Institute of Political Studies at the University of Tartu. She holds a PhD from the University of Arizona (2002). Her research focuses on elections, democracy and political attitudes in Europe, as well as aspects of European integration. Her work has appeared in the European Journal of Political Research, Cooperation and Conflict, Politics, Journal of Common Market Studies, and the Journal of Elections, Public Opinion & Parties, among others.

Mihkel Solvak holds a PhD in Political Science from Tartu University (2011) and is currently Associate Professor of Technology Research at the Johan Skytte Institute of Political Studies, University of Tartu, and head of the Center of IT-Impact Studies (CITIS). His research focuses on digitalization, digital service usage patterns, data driven e-services and Internet voting.

Jan Willemson defended his PhD in computer science at Tartu University, Estonia, in 2002. He has been working at Cybernetica as a researcher since 1998, specialising in information security and cryptography. His areas of interest include risk analysis of heterogeneous systems, secure multi-party computations, e-government solutions and security aspects of Internet voting. He has authored more than 60 research papers published in international journals and conferences.

Priit Vinkel holds a PhD in Public Administration from TalTech (2015) and has worked in the Estonian election management from 2005 to 2019. His last position was the Head of the Estonian State Electoral Office from 2013. He is currently engaged as an elections expert in national and international projects and employed as a part-time researcher at Cybernetica. His areas of interest focus on election administration and voting technologies.